WHAT IS CLAIMED IS:

1. A method for securely communicating via a network comprising:

receiving an input from a network multiplexer operable to identify an algorithm associated with a communication module;

processing information communicated between the communication module and the multiplexer using the network multiplexer using the identified algorithm.

2. The method of Claim 1, further comprising communicating an instruction to the communication module operable to identify the algorithm.

3. The method of Claim 2, further comprising:

receiving the instruction identifying the algorithm at the communication module; and

providing secure communication using the identified algorithm.

4. The method of Claim 1, further comprising:

providing a database associated with a central office; and

providing reference information associated with the network multiplexer in the database.

5. The method of Claim 4, further comprising:

determining subscribers and associated communication modules for the network multiplexer; and

updating the database based on the determined subscribers and communication modules.

6. The method of Claim 5, further comprising updating the database using information associated with a new communication module.

7. The method of Claim 6, further comprising identifying an algorithm associated with the new communication module.

8. The method of Claim 4, further comprising:

updating the database associated with the central office; and

synchronizing the central office database with a database operably associated with the network multiplexer.

9. The method of Claim 8, further comprising:

identifying communication modules associated with the network multiplexer; and

updating the network multiplexer database with reference information from the identified communication modules.

10. The method of Claim 1, further comprising:

determining a communication session between the communication module and the network multiplexer; and

processing information to provide the secure communication in response to determining the session.

11. The method of Claim 1, further comprising:

determining the algorithm operable to provide the secure communication;

communicating the algorithm to the communication module; and

storing the algorithm within a memory associated with the communication module.

12. A device operable to provide secure communication of information via a high speed network comprising:

a DSL modem operable to communicate with a DSLAM; and

a security module coupled to the DSL modem, the security module operable to provide secure communication of information between the DSL modem and the network DSLAM.

13. The device of Claim 12, wherein the security module comprises an algorithm operable to provide secure communication of information between the security module and the DSLAM.

14. The device of Claim 12, further comprising the DSL modem operable to receive an instruction from the DSLAM identifying an algorithm for use by the security module.

15. The device of Claim 12, wherein DSLAM comprises a reference operable to identify an algorithm associated with the DSL modem.

16. The device of Claim 12, wherein DSLAM comprises a DSLAM database operable to identify DSL modems operably associated with the DSLAM.

17. The device of Claim 16, wherein DSLAM database comprises subscriber information associated with the DSL

modems, the subscriber information including session information.

18. The device of Claim 12, wherein DSLAM is operably coupled to a central office, the central office including a central office database including DSLAM information and DSL subscriber information.

19. The device for Claim 12, further comprising memory operably coupled to the security module, the memory operable to store an algorithm communicated to the DSL modem.

20. A device for providing secure communication of information via a network comprising:

means for identifying an algorithm operable to provide the secure communication between a network multiplexer and a communication module; and

means for processing information communicated between the communication module and the network multiplexer using the algorithm.

21. The device of Claim 20, further comprising:

means for determining the algorithm using the network multiplexer; and

means for communicating an instruction to the communication module to identify the algorithm.

22. The device of Claim 21, further comprising:

means for receiving the instruction identifying the algorithm at the communication module; and

means for providing the secure communication based on the identified algorithm.

23. The device of Claim 20, further comprising:

means for providing a database associated with a central office; and

means for providing the database with reference information associated with the network multiplexer.

24. A medium including encoded logic for providing secure communication of information comprising the logic operable to:

identify an algorithm operable to provide a secure communication between a network multiplexer and a communication module; and

process information communicated between the communication module and the multiplexer using the algorithm.

25. The medium of Claim 24, further comprising the logic operable to:

receive an instruction identifying the algorithm; and

provide the secure communication based on the identified algorithm.

26. The medium of Claim 24, further comprising the logic operable to:

determine a communication session between the communication module and the network multiplexer; and

process information to provide the secure communication in response to determining the communication session.

27. The medium of Claim 24, further comprising the logic operable to:

receive the algorithm operable to provide the secure communication; and

store the algorithm within a memory associated with the communication module.